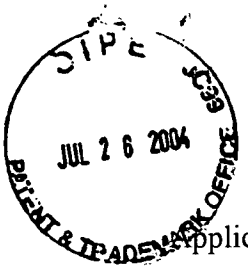
IFW

PATENT



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Sheueling Chang Shantz et al.

Title: METHOD AND APPARATUS FOR IMPLEMENTING PROCESSOR INSTRUCTIONS FOR ACCELERATING PUBLIC-KEY CRYPTOGRAPHY

Application No.:	10/789,311	Filed:	February 27, 2004
Examiner:	Not yet assigned	Group Art Unit:	2124
Atty. Docket No.:	004-30132		

July 21, 2004

Mail Stop Amendment
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT
37 C.F.R. § 1.97(b)

Dear Sir:

Pursuant to 37 C.F.R. § 1.56, § 1.97 and § 1.98, the undersigned brings the patents, publications, applications or other information identified in the attached:

☒ Form(s) PTO-1449 (1 pages), including copy(ies) of 14 reference(s).
☐ Other: n/a

to the Examiner's attention in the above-identified application. Citation of such information shall not be construed as:

1. an admission that the information necessarily is, or corresponds to, prior art with respect to the instant invention;
2. a representation that a search has been made, other than as described below; or
3. an admission that the information cited herein is, or is considered to be, material to patentability as defined in § 1.56(b).

Pursuant to 1276 OG 55 (August 5, 2003), Information Disclosure Statements may be filed without copies of U.S. Patents and Published Applications in Patent Applications filed after June 30, 2003.

For each item of information listed that is not in the English language, the undersigned has provided a concise explanation of the relevance through (i) an English language abstract, (ii) an English language equivalent application, or (iii) if cited in a search report or other action

by a foreign patent office in a counterpart foreign application, an English language version of the search report or action that indicates the degree of relevance found by the foreign office.

FEE AUTHORIZATION

☐ This Information Disclosure Statement is filed within three months of the filing date of a national application other than a continued prosecution application under § 1.53(d) or within three months of entry of the national stage as set forth in § 1.491 in an international application. Therefore, no fee is required.

☒ The undersigned believes that this Information Disclosure Statement is being filed before the mailing date of a first Office action on the merits or before the mailing date of a first Office action after the filing of a request for continued examination under § 1.114. Therefore, no fee is believed required.

If however, this Information Disclosure Statement is filed after the period specified in § 1.97(b), the undersigned hereby authorizes the Commissioner to charge the fee set forth in § 1.17(p) to Deposit Account No. 50-0631.

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that, on the date shown below, this correspondence is being

☒ deposited with the US Postal Service with sufficient postage as first class mail, in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

☐ facsimile transmitted to the US Patent and Trademark Office.

Mark Zagorin — 7/21/07
Mark Zagorin — Date

EXPRESS MAIL LABEL: _____

Respectfully submitted,

Mark Zagorin, Reg. No. 36,067
Attorney for Applicant(s)
(512) 338-6311
(512) 338-6301 (fax)

U.S. Department of Commerce, Patent and Trademark Office	**Attorney Docket No.:**	*004-30132*
	Application No.:	*10/789,311*
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	**Applicant(s):**	*Sheueling Chang Shantz et al.*
(Use several sheets if necessary)	**Filing Date:**	*February 27, 2004*
	Group Art Unit:	*2124*
	Date Submitted:	July 21, 2004

NON PATENT LITERATURE DOCUMENTS

*Examiner Initial	Cite No.	(Including name of author in capital letters, title of article, title of item, date, pertinent pages, volume-issue number(s), publisher, city and/or country where published.)
/CJ/	AA	Intel® Itanium™ Processor, "High Performance On Security Algorithms (RSA Decryption Kernel)," Intel Corporation, 2001, pp. 1-8.
	AB	Intel®, "Intel® Itanium™ Architecture Software Developer's Manual, Volume 1: Application Architecture," Revision 2.1, October , 2002, 2 pages.
	AC	Cohn, Leonard Allen, "Generate-Propagate Adders," ChoPP Computer Corporation, prior to 2000, pp. 1-16.
	AD	Fairchild, "F100K ECL Data Book," Fairchild Camera and Instrument Corporation, 1982, pp. 3-177 – 3-178.
	AE	Großschädl, Johann, "Instruction Set Extension for Long Integer Modulo Arithmetic on RISC-Based Smart Cards," Proceedings of the 14th Symposium on Computer Architecture and High Performance Computing, 2002, 7 pages.
	AF	Koç, Cetin Kaya, "High-Speed RSA Implementation," Version 2.0, RSA Laboratories, November, 1994, pp. i-70.
	AG	Mano, M. Morris, "Computer System Architecture," Prentice-Hall, Inc., 1976, pp. 244-249.
	AH	Shantz, Sheueling Chang, "From Euclid's GCD to Montgomery Multiplication to the Great Divide," Sun Microsystems, June 2001, pp. 1-10.
	AI	Standards for Efficient Cryptography, "SEC 2: Recommended Elliptic Curve Domain Parameters," Certicom Research, September 20, 2000, pp. i-45.
	AJ	Woodbury, A.D.; Bailey, Daniel V., Paar, Christof, "Elliptic Curve Cryptography on Smart Cards Without Coprocessors," The Fourth Smart Card Research and Advanced Applications (CARDIS2000) Conference, Bristok, UK, pp. 71-92.
	AK	H. Cohen, A. Miyaji, and T. Ono, "Efficient elliptic curve exponentiation using mixed coordinates", in K. Ohta and D. Pei, editors, Advances in Cryptology ASIACRYPT 98, pp. 51-65, Springer Verlag, 1998, LNCS 1514
	AL	D. Bailey and C. Paar, "Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms." In H. Krawczyk, editor, Advances in Cryptography – CRYPTO '98, volume LNCS 1462, pages 472-485. Springer-Verlag, 1998. http://citeseer.ist.psu.edu/article/bailey98optimal.html, 14 pages.
	AM	H. Pietiläinen, "Elliptic Curve Cryptography on Smart Cards," Master's Thesis, Helsinki University of Technology, Oct. 12, 2000, pp. i-81.
	AN	F. Morain and J. Olivos, "Speeding Up the Computations on an Elliptic Curve Using Addition-Subtraction Chains," Rapport de Recherche 983, INRIA, France, March 1989, http://citeseer.ist.psu.edu/morain90speeding.html, pp. 119-130.
	AO	
	AP	
	AQ	

Examiner /Carlton Johnson/	**Date Considered** 06/09/2007

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with your communication to applicant.